Universidade do Porto

Faculdade de Engenharia

FEUP

Segurança em Sistemas Informáticos

Autoridade de Certificação

João Brito - 070509052

João Coelho - 070509118

Índice

Índice 3
Introdução 4
Problema 5
Objectivos 5
Enquadramento Teórico 6
  Autoridade Certificadora 6
  Certificado Digital 6
Estado da Arte 8
  OpenCA 8
  PHPki 8
  EJBCA 9
Instalação do EJBCA 10
Perspetivas de Solução 11
  Implementação da CA na Universidade do Porto 12
  Inscrição dos utilizadores 13
  Certificados para browser – autenticação do utilizador 15
  Certificados para browser – SSL 15
  Certificados – outras aplicações 18
  Validação de assinaturas 19
  Expiração das chaves 20
  Listas de revogação 20
  Documentação para o utilizador 21
Conclusão 22
Bibliografia 23

Introdução

Numa sociedade cada vez mais dependente de tecnologias de informação, a comunicação tem cada vez maior importância e, como tal, existe uma necessidade cada vez maior de confiar na veracidade da mesma. Esta realidade está especialmente presente em instituições públicas e privadas que intercomunicam vastamente com os seus colaboradores através de e-mail ou outro tipo de ferramentas.

A infra-estrutura oferecida pelos certificados digitais permite elevar o nível de confiança entre entidades comunicantes. Ao nível da Universidade do Porto, e mais concretamente na Faculdade de Engenharia da Universidade do Porto, ainda não está implementado nenhum mecanismo de certificação de informação.

É neste contexto que o presente documento é elaborado, descrevendo uma metodologia fácil e de baixo custo para implementação de uma autoridade de certificação centralizada que servisse para certificar informação e, principalmente, intervenientes envolvidos.

Problema

Existe a necessidade de implementar uma autoridade de certificação com abrangência a toda a Faculdade de Engenharia e, possivelmente, à própria Universidade do Porto. Esta entidade será responsável pela emissão de certificados digitais aos utilizadores pertencentes à rede.

O sistema deverá ser genérico para poder ser usado para um conjunto variado de contextos, como e-mail, repositórios de ficheiros, comunicações oficiais, etc..

Um dos requisitos adicionais passa por definir de forma clara todos os processos inerentes ao funcionamento de uma CA para que os responsáveis pela real implementação do sistema tenham acesso a um manual prévio de boas práticas. Para os utilizadores comuns da ferramenta existe a vantagem de terem acesso a um manual de utilizador de fácil leitura.

Objectivos

Apresentado o problema, apresentam-se de seguida os objectivos do presente trabalho:

1. Breve apresentação da **moldura teórica** inerente aos certificados digitais;

2. Estudar e discutir o **estado de arte**, ou seja, analisar a viabilidade de várias soluções open source que implementem Autoridades de Certificação;

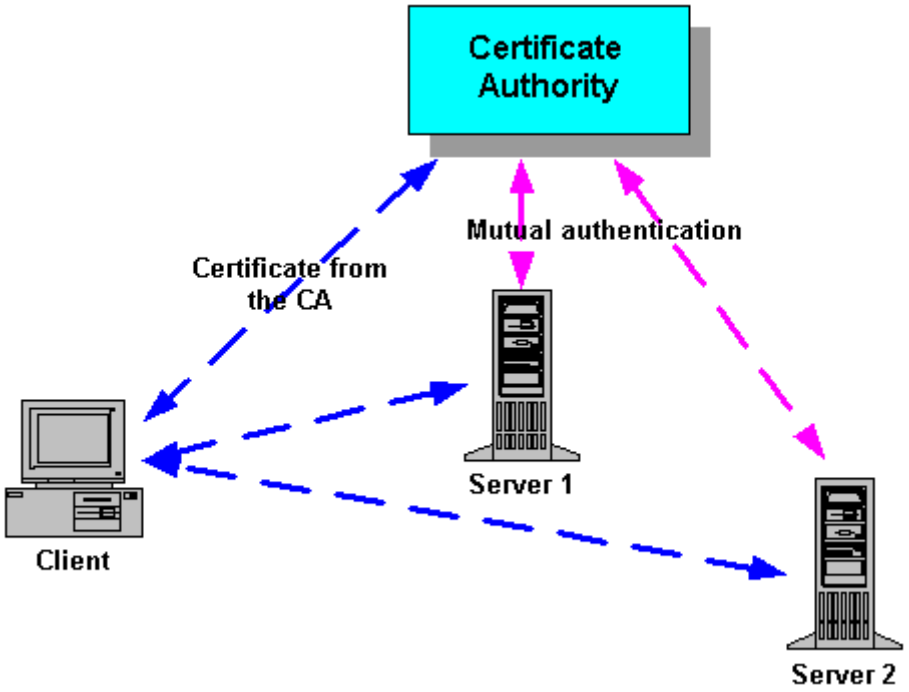
3. Escolher a **tecnologia mais viável**, documentá-la de forma a ser possível a terceiros replicar os processos descritos, apresentando um manual de instalação e configuração do sistema;

4. Apresentação e análise de um **conjunto de casos** de uso do sistema e enquadramento dos mesmos com exemplos de utilização da CA;

Enquadramento Teórico

Autoridade Certificadora

Resumidamente, uma autoridade de certificação apresenta-se como uma entidade externa cujo objectivo é o de promover confiança entre duas entidades comunicantes.



Em criptografia, uma CA é responsável por gerir informação sobre os clientes, e emitir certificados digitais que podem ser usados para validar dados transmitidos. Desta forma, ao assinar um documento, um utilizador consegue identificar-se de forma genuína e os destinatários conseguem saber com certeza que o documento é realmente da autoria dessa pessoa. Além do mais, o documento assinado não poderá ser posteriormente repudiado.

Certificado Digital

Como foi referido anteriormente, as entidades certificadoras emitem certificados digitais, que correspondem a documentos onde se indicam os dados individuais da pessoa e a chave pública a ser usada para verificar assinaturas posteriores dessa mesma pessoa.

Tipicamente, o autor da informação obtém um *fingerprint* da mesma, cifrando-a com a sua chave privada. Posteriormente, ao publicar os dados, publica também a sua assinatura

(hash do documento cifrado) para que os destinatários possam verificar a validade da publicação com a chave pública previamente disponibilizada.

O problema surge quando um utilizador mal intencionado consegue fazer outros acreditar que a chave pública é outra; a partir deste momento, ele pode assinar documentos falsos com a sua chave privada e fazer os destinatários acreditar na validade da informação. É por esta razão que é vital a existência de entidades certificadoras centrais que sejam responsáveis por validar as chaves públicas detidas pelos utilizadores.

Pode acontecer que uma determinada chave pública seja revogada por ter sido violada ou simplesmente por a informação do dono ter sido modificada. É, por isso, essencial que a CA possua mecanismos de divulgação de chaves revogadas. O utilizador também deve ter em atenção a validade dos certificados que tem em sua posse.

Todos estes aspectos têm muita importância na implementação da entidade certificadora, para que utilizadores fraudulentos não sejam capazes de se aproveitar do sistema.

Estado da Arte

OpenCA

No sentido de analisar a melhor tecnologia *opensource* presente no mercado, fez-se uma pesquisa no Google tendo-se encontrado muita referência ao OpenCA. A página oficial do projecto está localizada no seguinte endereço: http://www.openca.org/.

O openCA corre sobre um servidor Apache, com auxílio de ferramentas como PHP e Perl. Verificou-se que a instalação do software é ardilosa e muito pouco documentada. Apesar de se conseguir colocar uma CA a funcionar com base nesta tecnologia, a sua ineficiência pode tornar cara a manutenção a longo prazo do serviço.

OpenCA
http://www.openca.org
Email | Print
PKI Info
My Certificates
Information
Help
Languages
Home
Request a Certificate
To request a certificate use one of this links. You will be asked to fill in a form and to confirm inserted data. After having completed the request you will have to go to the chosen RA for request approval.
Browser Certificate Request
Request form with automatic browser detection
Authenticated Browser Certificate Request
Request form with automatic browser detection
Server Certificate Request
PKCS#10 PEM formatted Request Upload Form
Search
OpenCA Software © 1998-2010 by Massimiliano Pala and the OpenCA Labs.

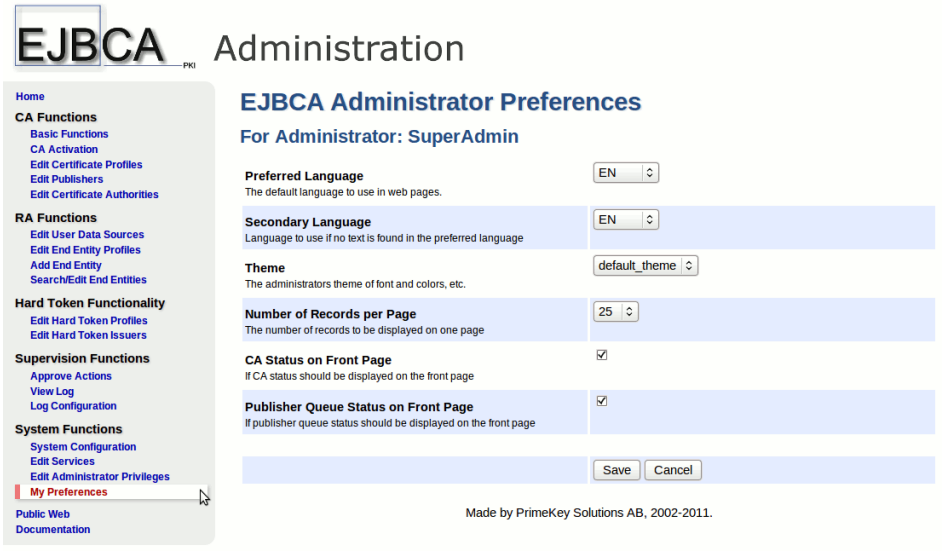
PHPki

O PHPki é uma ferramenta totalmente escrita em PHP. Só requer a existência de um sistema operativo Linux, com um servidor Apache e PHP incorporados para se usar. Contudo, o sistema só é feito para ser usado para certificação de e-mail. Como o objectivo inicial do trabalho seria o de desenvolver uma arquitectura genérica que pudesse ser usada em qualquer contexto, também se acabou por colocar de parte esta ferramenta.

EJBCA

Esta ferramenta tem algumas características interessantes. Em primeiro lugar, ao invés de estar assente numa arquitectura Apache, baseia-se num servidor aplicacional derivado do Java, o JBOSS. Uma das principais vantagens passa por ser possível implementar uma CA num dos variados sistemas operativos existentes.

Por outro lado, verificou-se que é de mais fácil instalação e configuração. Por estas razões **recomenda-se a utilização desta ferramenta**. A título de exemplo, optou-se por instalar o EJBCA em ambiente Linux (ubuntu “edição feup”).



Instalação do EJBCA

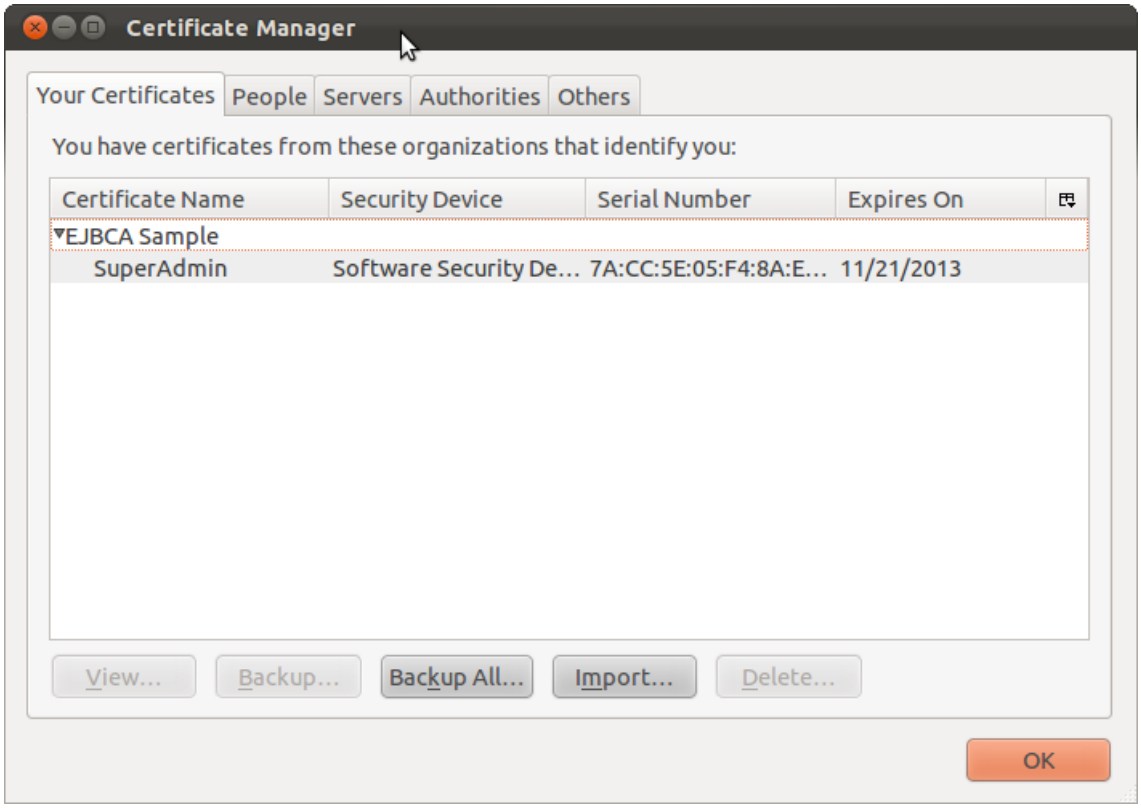
1. Instalar e configurar correctamente o Ubuntu “Edição FEUP”;
2. *su “nome do utilizador”*
    a. “password”
3. Fazer download do sourceforge dos seguintes pacotes:
    a. jboss-5.1.0.GA-jdk6.zip
    b. ejbca_4_0_5.zip
4. Utilizar o apt-get para instalar programas acessórios necessários:
    a. sudo apt-get install openjdk-6-jdk ant ant-optional unzip ntp
5. Descompactar ficheiros em 2) para a pasta *user*
6. Configurar o EJBCA para conseguir encontrar o servidor aplicacional JBOSS
    a. echo "appserver.home=/home/user/jboss-5.1.0.GA" >> ejbca_4_0_6/conf/ejbca.properties
7. Integrar EJBCA no JBOSS
    a. cd ejbca_4_0_6
    b. ant bootstrap
8. Abrir terminal e correr JBOSS
    a. jboss-5.1.0.GA/bin/run.sh
9. Abrir terminal e correr o seguinte comando para criar novo administrador da CA
    a. ant install
    b. (escolher valores por pré definição para teste, ou ajustar consoante os requisitos)
    c. ant deploy
10. Reiniciar JBOSS
    a. ctrl-c
    b. jboss-5.1.0.GA/bin/run.sh

Perspetivas de Solução

O EJBCA tem uma arquitectura que permite uma utilização independente por parte de administradores e utilizadores normais. Para se ter acesso à secção administrativa, deve-se ter instalado um certificado específico no browser. O administrador pode encontrá-lo na **pasta do EJBCA, na directoria *p12***:

/home/user/ejbca_4_0_6/p12/superadmin.p12

Tal como é mostrado na imagem abaixo, é necessário importar o certificado para a secção "Os seus certificados" (firefox).

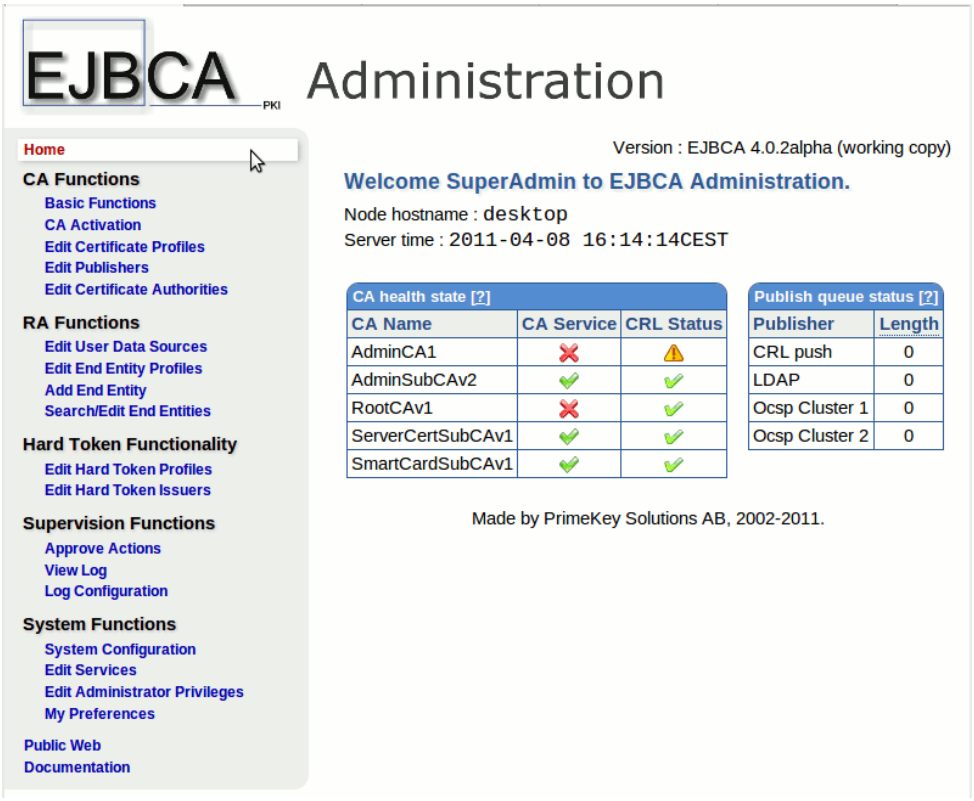


Depois de efectuado este processo, o administrador pode aceder ao seguinte endereço, correspondente à administração:

https://localhost:8443/ejbca/adminweb

As principais funcionalidades disponibilizadas nesta área são as seguintes:

- Criação e activação de CA's;
- Criação e edição de entidades na CA;
- Gestão dos recursos da CA;
- Criação e edição de perfis de certificados;



Por outro lado, o utilizador pode querer aceder à autoridade certificadora para verificar se um certificado foi revogado, ou até para introduzir um novo par de chaves. Para o fazer, pode aceder à seguinte URL:

https://localhost:8443/ejbca

As principais funcionalidades disponibilizadas nesta área são as seguintes:

- Adição de pares de chaves para uma entidade;
- Verificação se um certificado foi revogado;

Implementação da CA na Universidade do Porto

Depois de instalada e configurada, a CA deverá ser publicada na Web para que qualquer pessoa lhe consiga aceder através de uma ligação SSL. Propõe-se o uso de um subdomínio para a navegação ser fácil através do browser (p.e. certaut.up.pt).

Todas as faculdades seriam responsáveis por colocar um apontador nos seus websites para a CA. A responsabilidade pela gestão do serviço estaria a cargo do CICA.

Por outro lado, alerta-se para o facto de a instalação apresentada anteriormente ser a instalação de teste, com valores pré definidos. No caso de ser implementado este sistema para a Universidade do Porto, dever-se-á ter em consideração a atribuição de dados específicos aquando da execução do comando "*ant install*".

Na instalação, é importante definir o CN de forma correcta, para que este identifique a Universidade do Porto de forma inequívoca.

Inscrição dos utilizadores

A inscrição de novos utilizadores é um dos passos mais importantes. Isto porque quem opera a CA deve certificar-se que quem está a certificar é mesmo quem diz ser. Na FEUP, quando o aluno se inscreve pela primeira vez, é necessário que apresente documentação que prove a sua identidade. Sugere-se, por isso, que aquando da inscrição do aluno na faculdade em questão, o administrativo também registe o utilizador na CA.

Para outros casos, como professores ou outros profissionais que queiram inscrever-se na CA, devem dirigir-se ao CICA para apresentar a documentação necessária. De seguida apresenta-se uma proposta das provas que devem ser apresentadas (mínimo indispensável):

- **Cartão de Cidadão** ou **Bilhete de Identidade**

Assim que se prova a própria identidade junto de uma pessoa autorizada a trabalhar com a parte administrativa do EJBCA, deve-se iniciar o processo de registo do utilizador. Como a conta de e-mail é gerida internamente pelo CICA, a partir da prova de identidade pode-se provar-se a validade do e-mail, pelo que não se considera necessário ter que apresentar nenhuma prova adicional.

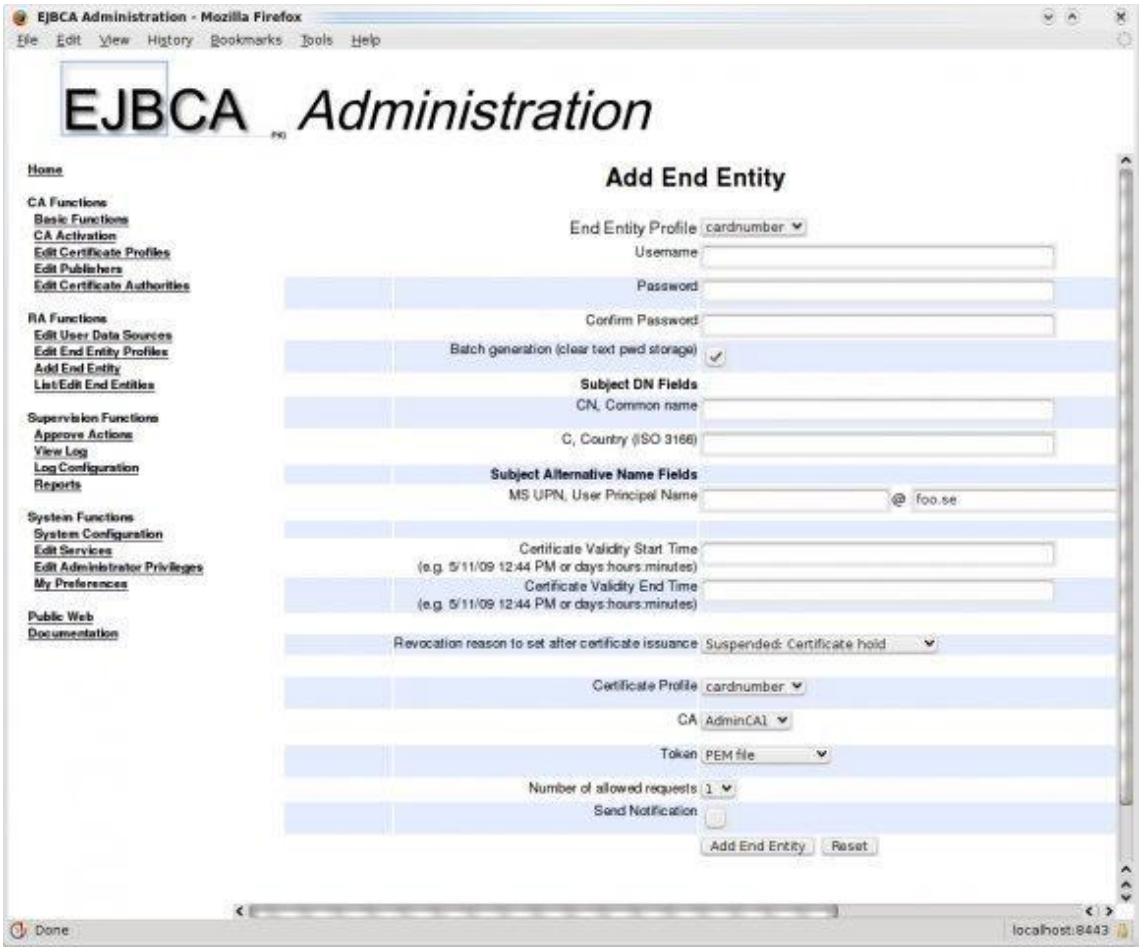
Para casos especiais de pessoas que desejem validar o número de telefone, morada ou e-mail externo à instituição, sugerem-se rotinas de certificação adicionais.

Número de telefone/telemóvel e e-mail: o utilizador deverá requerer um código especial no site do sigarra antes de se apresentar no CICA. Se pedir esse código para um número de telefone ou telemóvel, deverá aguardar por uma chamada onde lhe deve ser indicado o referido código secreto. Posteriormente, deverá apresentar a senha no CICA. O administrativo, após confirmar a validade da senha, poderá então editar a conta do utilizador no EJBCA, introduzindo o registo pessoal adicional. Para caso de e-mails externos, o processo é semelhante com a diferença que o código deverá ser enviado para o e-mail pedido. NOTA: este

processo não verifica totalmente os dados, apenas prova que o utilizador consegue aceder aos serviços que tenta certificar. Todavia, actualmente é o processo mais utilizado em inúmeros contextos e é globalmente aceite como sendo suficiente.

Morada: para certificar o acesso a uma morada, o requerente deverá apresentar no CICA um comprovativo de morada (conta da água ou luz, por exemplo). Este comprovativo deverá vir endereçado à pessoa em questão.

Como se pode ver na imagem abaixo, pode-se criar uma entidade com o objectivo pretendido, bastando escolher o tipo de perfil que se quer.



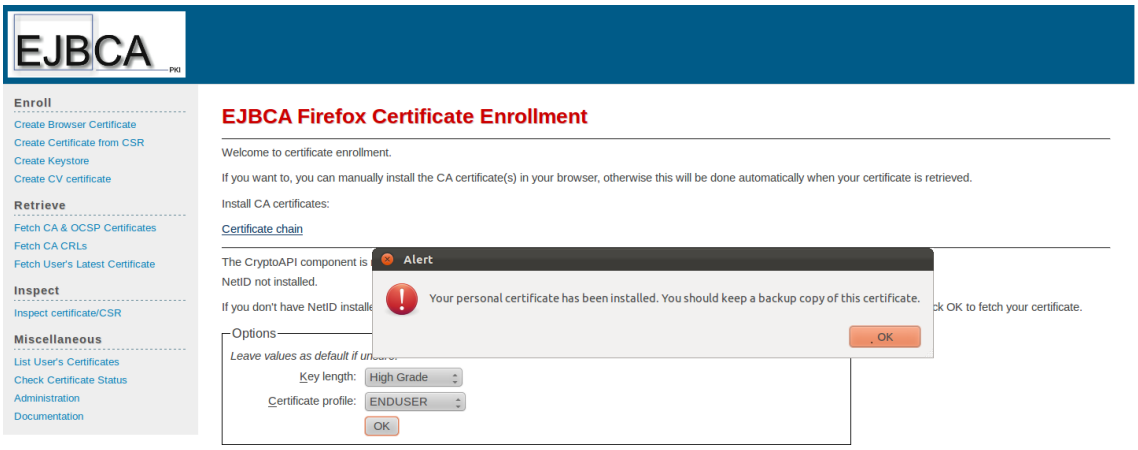
No EJBCA, o utilizador registado passa a ter um *username* e uma *password* que pode usar para fazer pedidos específicos. Pode inclusivamente usar esses dados para registar novas chaves criptográficas geradas por si. No momento do registo, o utilizador deverá escolher uma password que só ele conheça. O administrativo do CICA deverá enviar-lhe para o e-mail um ficheiro do tipo p12 (que é protegido por palavra-chave) com um par criptográfico inicial. A password do ficheiro é a que o utilizador escolheu.

O utilizador registado pode usar o certificado do tipo p12 para assinar e-mail, ficheiros ou outro tipo de documentos.

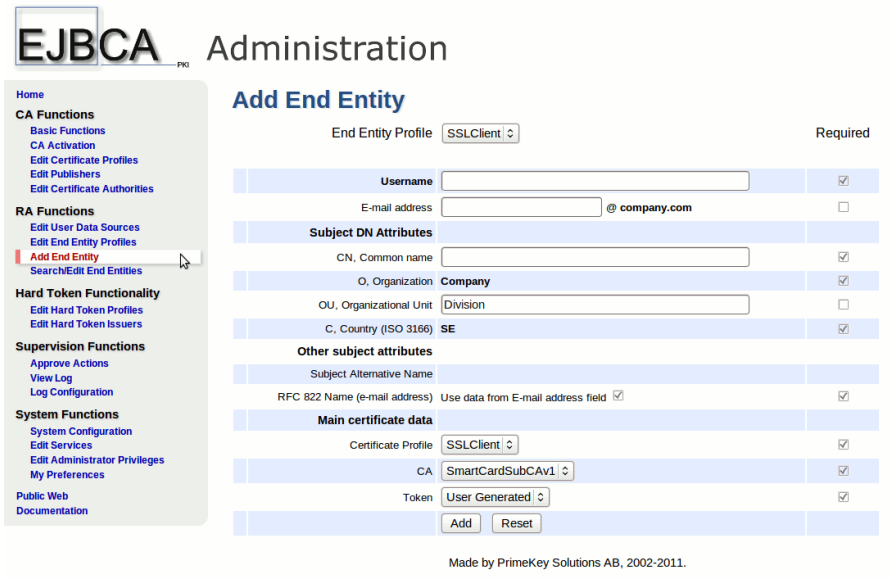
Certificados para browser – autenticação do utilizador

Certificar um utilizador na sua navegação habitual na Web sem que o mesmo tenha que introduzir nome de utilizador e password é de extrema importância. Pode-se aplicar este critério de autenticação no acesso ao *sifeup*, *feupload* ou *webmail*.

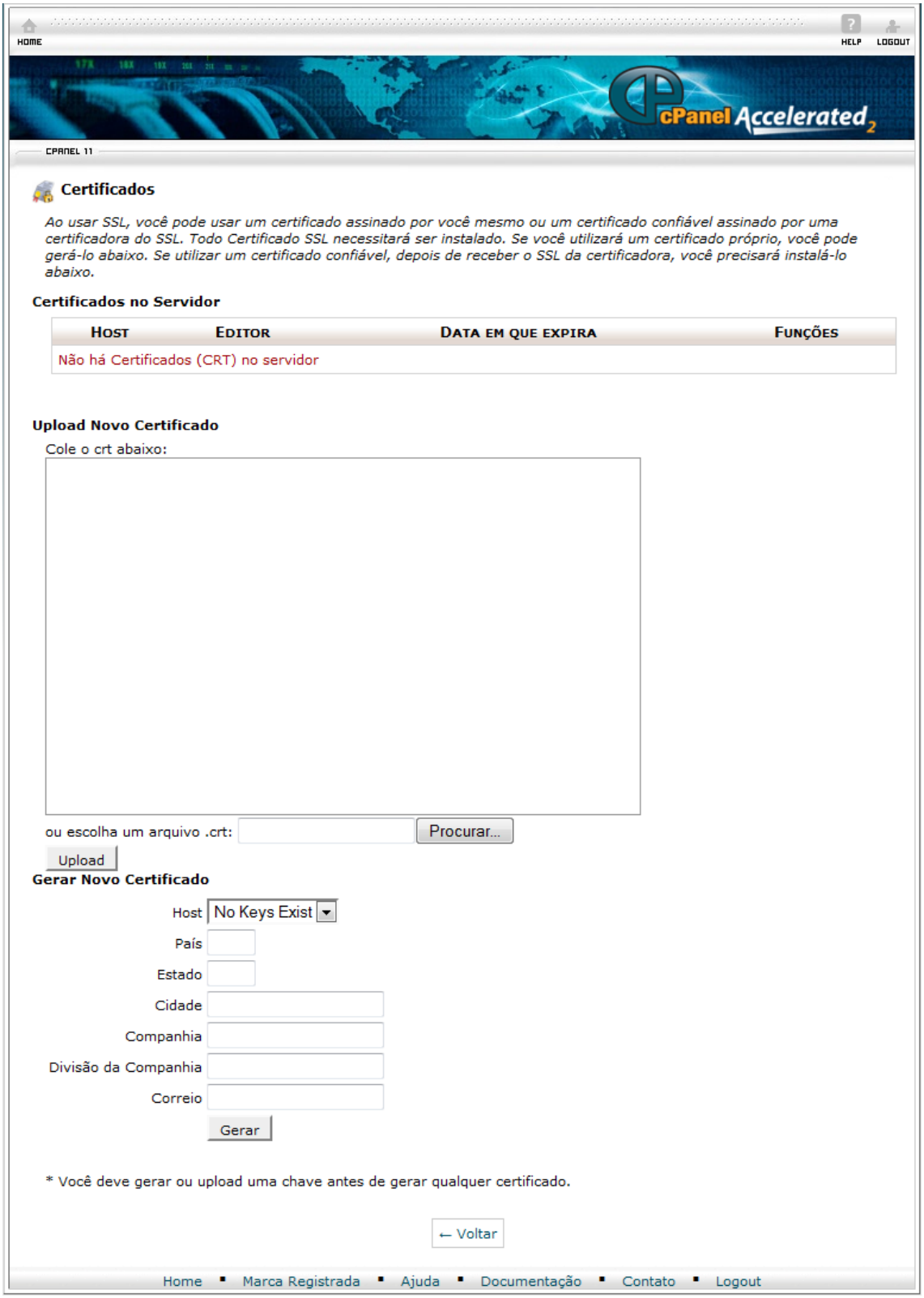
A aplicação do lado do servidor terá que ser capacitada para comunicar com a CA frequentemente para actualizar as suas listas de revogação para impedir o acesso a utilizadores cujos certificados tenham expirado.



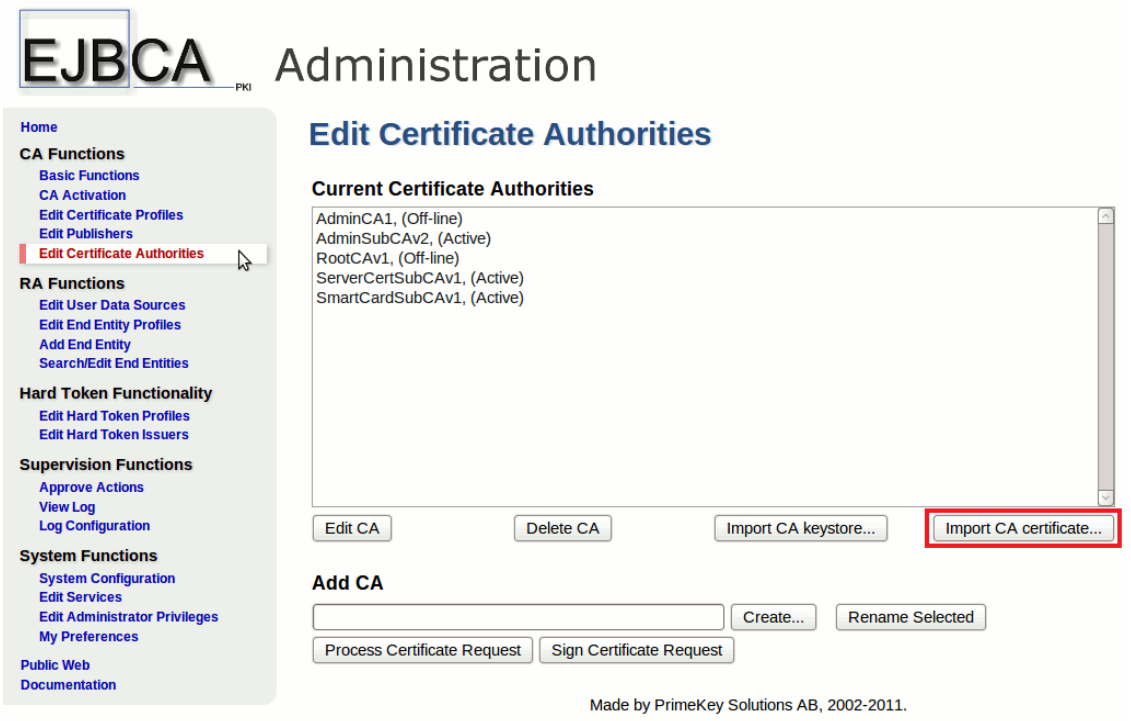
Certificados para browser – SSL



O EJBCA permite a criação de certificados para certificar ligações SSL. Este tipo de certificados pode ser importante para serviços específicos ou projectos académicos dos estudantes e professores. Depois de criado, o certificado pode ser importado em aplicações como o cpanel (como se mostra na figura abaixo).



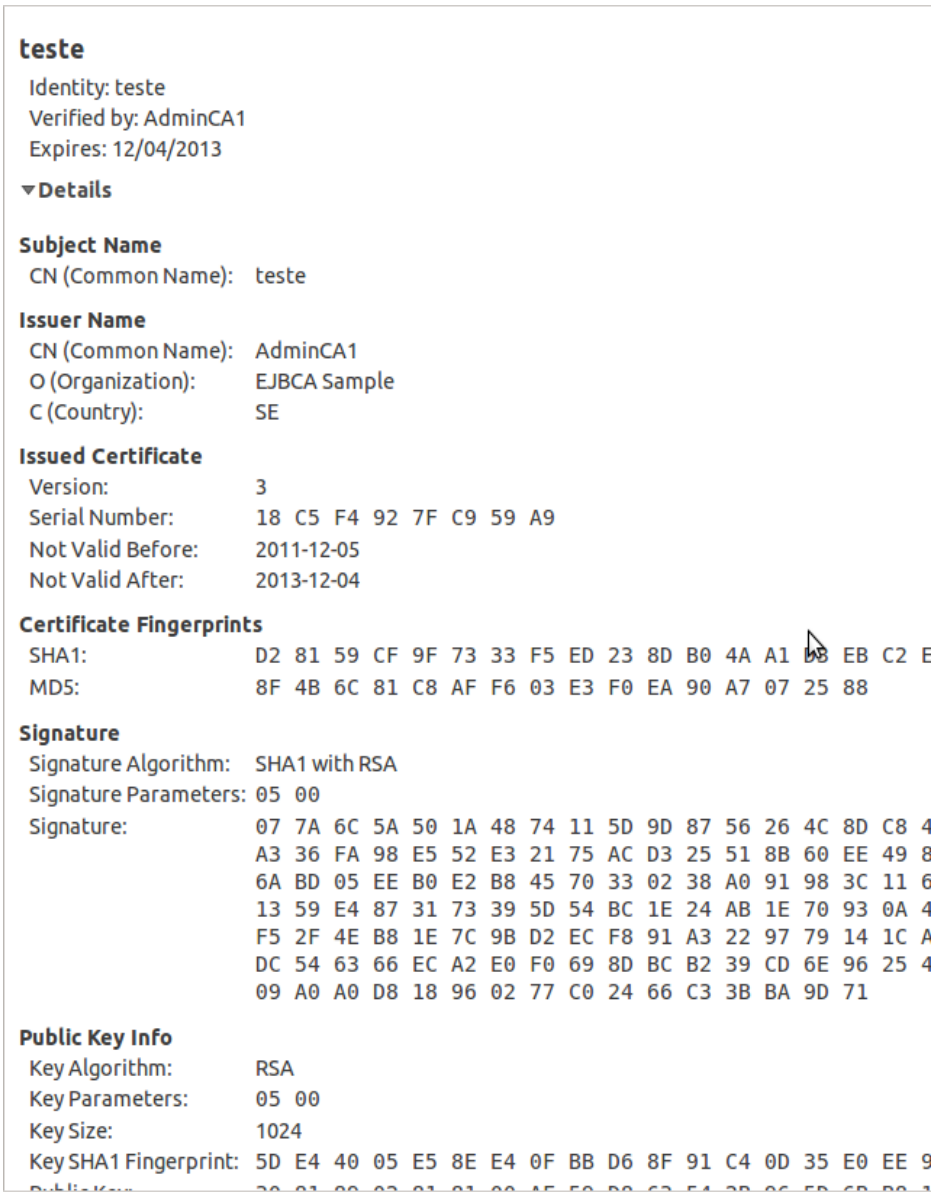
Indica-se que, para os certificados terem validade, os utilizadores devem ser encorajados a instalar nos browsers pessoas o certificado *root* da CA "certaut.up.pt". Sugere-se que possa ser feito download do certificado root no site do sigarra (apesar de estar presente para download em *certaut.up.pt)*.



Certificados – outras aplicações

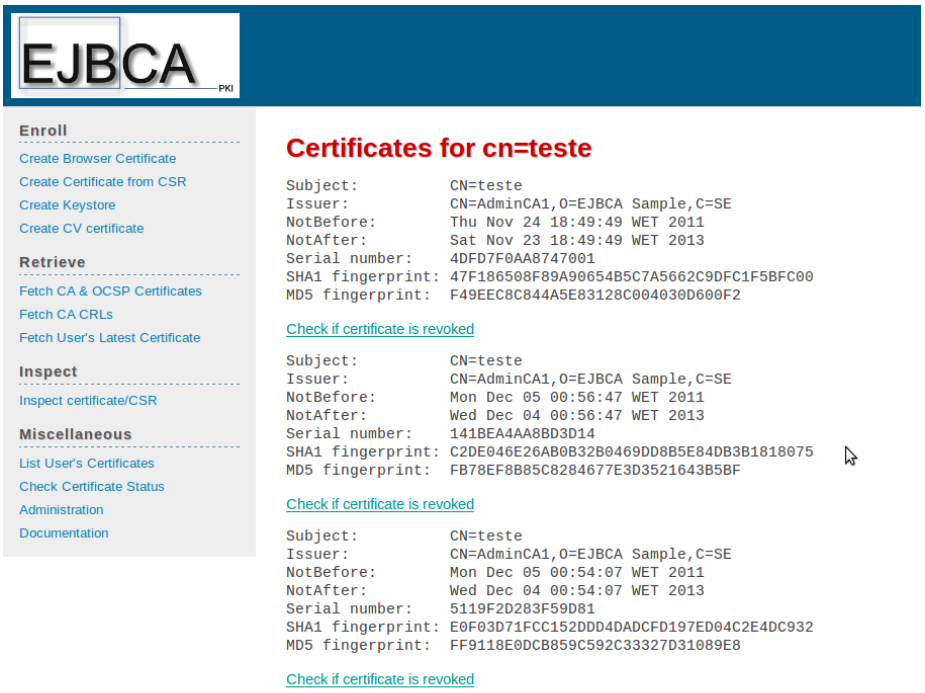
A partir do momento que o utilizador tem em sua posse as chaves criptográficas pode usá-las para assinar e-mail, documentos ou outro tipo de informação. Basta para isso usar software já existente, como um serviço de e-mail que suporte assinaturas digitais. O software usado para assinar a informação não é relevante. O que importa é que a assinatura seja enviada com a chave pública para ser possível validar a informação.

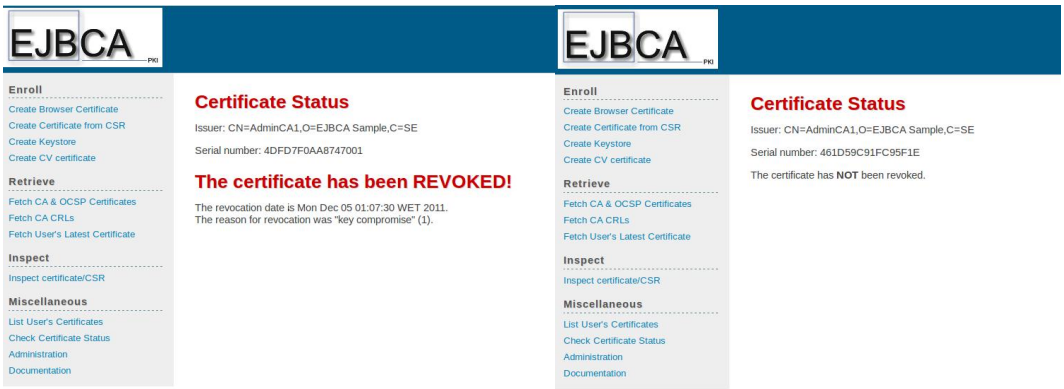
As chaves públicas devem ser registadas na CA previamente, sendo posteriormente devolvido um certificado que pode ser tornado público. Na imagem seguinte mostra-se um exemplo de um certificado gerado a partir de um CSR.


teste
Identity: teste
Verified by: AdminCA1
Expires: 12/04/2013
Details
Subject Name
CN (Common Name): teste
Issuer Name
CN (Common Name): AdminCA1
O (Organization): EJBCA Sample
C (Country): SE
Issued Certificate
Version: 3
Serial Number: 18 C5 F4 92 7F C9 59 A9
Not Valid Before: 2011-12-05
Not Valid After: 2013-12-04
Certificate Fingerprints
SHA1: D2 81 59 CF 9F 73 33 F5 ED 23 8D B0 4A A1
MD5: 8F 4B 6C 81 C8 AF F6 03 E3 F0 EA 90 A7 07 25 88
Signature
Signature Algorithm: SHA1 with RSA
Signature Parameters: 05 00
Signature: 07 7A 6C 5A 50 1A 48 74 11 5D 9D 87 56 26 4C 8D C8 4
A3 36 FA 98 E5 52 E3 21 75 AC D3 25 51 8B 60 EE 49 8
6A BD 05 EE B0 E2 B8 45 70 33 02 38 A0 91 98 3C 11 6
13 59 E4 87 31 73 39 5D 54 BC 1E 24 AB 1E 70 93 0A 4
F5 2F 4E B8 1E 7C 9B D2 EC F8 91 A3 22 97 79 14 1C A
DC 54 63 66 EC A2 E0 F0 69 8D BC B2 39 CD 6E 96 25 4
09 A0 A0 D8 18 96 02 77 C0 24 66 C3 3B BA 9D 71
Public Key Info
Key Algorithm: RSA
Key Parameters: 05 00
Key Size: 1024
Key SHA1 Fingerprint: 5D E4 40 05 E5 8E E4 0F BB D6 8F 91 C4 0D 35 E0 EE 9

Validação de assinaturas

Assim que a informação chega ao destinatário, pode ser verificada. É importante que a CA tenha a ferramenta de verificar a validade de um certificado. O EJBCA tem essa capacidade, por isso o utilizador pode importar periodicamente listas de certificados revogados. O utilizador deve ser dado a conhecer a importância de fazer actualização das CLR para garantir a segurança do sistema.





Expiração das chaves

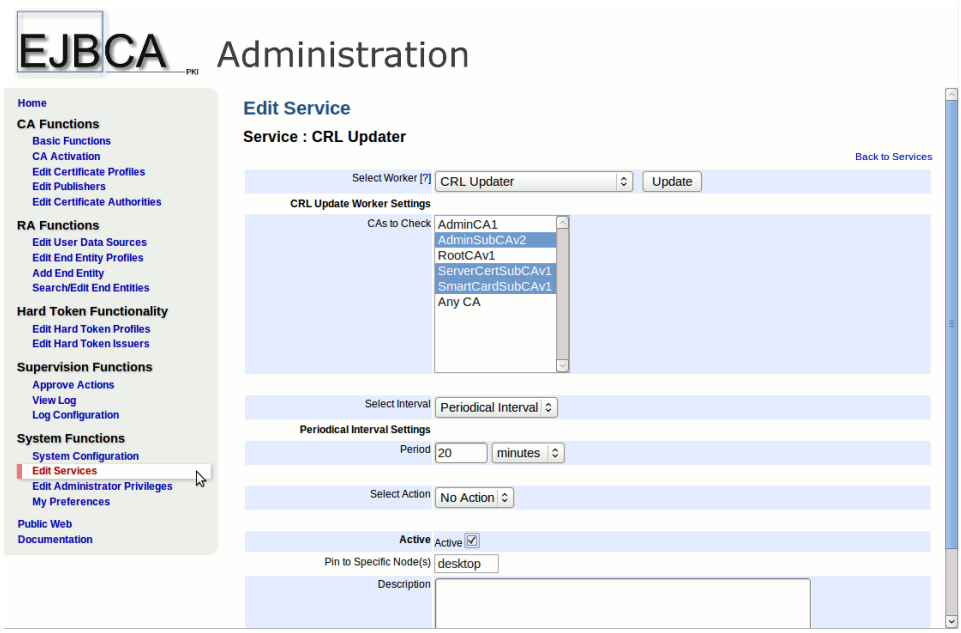
A CA deverá emitir certificados aos alunos com uma validade que não exceda o tempo de curso. Caso um aluno ou outro utilizador veja as suas chaves expiradas, deverá dirigir-se ao CICA e pedir para lhe serem geradas outras chaves. Ou em alternativa pode, ele próprio, gerar as novas chaves e introduzi-las na CA, usando o seu login. Deve ter em atenção que o pedido deve ser um CSR codificado em Base64.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBnTCCAQYCAQAwXTELMAkGA1UEBhMCU0cxETAPBgNVBAoTCE0yQ3J5cHRvMRIw
EAYDVQQDEwlsb2NhbGhvc3QxJzAlBgkqhkiG9w0BCQEWGGFkbWluQHNlcnZlci5l
eGFtcGxlLmRvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAr1nYY1Qrll1r
uB/FqlCRrr5nvupdIN+3wF7q915tvEQoc74bnu6b8IbbGRMhzdzmvQ4SzFfVEAuM
MuTHeybPq5th7YDrTNizKKxOBnqE2KYuX9X22A1Kh49soJJFg6kPb9MUgiZBiMlv
tb7K3CHfgw5WagWnLl8Lb+ccvKZZl+8CAwEAAaAAMA0GCSqGSIb3DQEBBAUAA4GB
AHpoRp5YS55CZpy+wdigQEwjL/wSluvo+WjtpvP0YoBMJu4VMKeZi405R7o8oEwi
PdlrrliKNknFmHKIaCKTLRcU59ScA6ADEIWUzqmUzP5Cs6jrSRo3NKfg1bd09D1K
9rsQkRc9Urv9mRBIsredGnYECNeRaK5R1yzpOowninXC
-----END CERTIFICATE REQUEST-----
```

A CA deverá validar o pedido e mais tarde devolver um certificado assinado por si com a informação pedida (caso esta seja igual à que já está registada na BD). O utilizador poderá depois publicar esse mesmo certificado onde desejar.

Listas de revogação

O EJBCA oferece a possibilidade de definir a frequência de actualização das CRL. Cabe à administração determinar as melhores definições.



Documentação para o utilizador

Não se deve esquecer ainda que o sigarra deverá ter uma página onde descreva de forma bastante sucinta os passos que o utilizador deve fazer para conseguir utilizar a *certaut*. As recomendações poderão basear-se neste documento, contudo deverão ser estendidas de forma a explicar um pouco como o utilizador pode gerar CSR ou assinar documentos, utilizando software grátis já existente, como *openpgp* ou *openssl*.

Conclusão

As autoridades de certificação desempenham um papel muito importante na promoção de confiança entre partes comunicantes. Com o presente trabalho, apresentou-se uma proposta de arquitectura e implementação de uma autoridade certificadora própria da Universidade do Porto.

Relembra-se que o software discutido ainda não é totalmente confiável de instalar. O EJBCA é o que oferece mais garantias. Contudo, não se espere que a configuração de uma CA seja uma tarefa fácil. A instalação do software flutua muito de sistema para sistema o que trará grandes dificuldades para o administrador.

Talvez seja por esta razão que ainda são pouco usadas soluções neste tipo de bases *opensource*. Ainda assim, pensa-se que se conseguiu um trabalho satisfatório que poderá servir de fundação e apoio à implementação da entidade certificadora na Universidade do Porto.

Bibliografia

- **Autoridade de Certificação** - http://pt.wikipedia.org/wiki/Autoridade_de_Certifica%C3%A7%C3%A3o

- **Modelo X.509** - http://en.wikipedia.org/wiki/X.509

- **Certificado Digital** - http://pt.wikipedia.org/wiki/Certificado_digital

- **Ferramentas**

  - **Webiste Oficial do OpenCA** - http://www.openca.org/

  - **Website Oficial do EJBCA** - http://www.ejbca.org/

  - **Website Oficial do PHPki** - http://sourceforge.net/projects/phpki/